Приложение 7

к Условиям дистанционного банковского обслуживания (система «ВТБ Бизнес»)

Рекомендации по обеспечению информационной безопасности при работе в системе «ВТБ Бизнес»

Важнейшим фактором, способствующим обеспечению безопасности, является личная заинтересованность Клиента. Банк считает необходимым соблюдение Клиентами следующего комплекса мер по защите информации:

1. Требования по обеспечению безопасности компьютера, с которого осуществляется работа в системе «ВТБ Бизнес»

1.1. Компьютеры должны располагаться в помещениях, обеспечивающих невозможность несанкционированного доступа к ним или должен быть обеспечен режим эксплуатации компьютера, исключающего доступ к нему неуполномоченных лиц.

1.2. Правом доступа к компьютерам должны обладать только лица, ознакомленные с настоящими требованиями и с другими нормативными документами, регламентирующими работу в ИБ «ВТБ Бизнес».

1.3. Запрещается оставлять без контроля компьютер при включенном питании и загруженном программном обеспечении. При кратковременном перерыве в работе следует блокировать сессию пользователя в операционной системе, возобновление активности сессии пользователем должно производиться с использованием пароля доступа.

1.4. Рекомендуется подключать компьютер к сети электропитания через устройства бесперебойного питания.

1.5. Установите и регулярно обновляйте лицензионное программное обеспечение, а также антивирусное программное обеспечение на вашем компьютере. Действие вредоносных программ может быть направлено на перехват вашей персональной информации и передачу ее третьим лицам.

1.6. Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполняйте обновления (патчи) операционной системы и браузера вашего компьютера, что значительно повысит его уровень безопасности.

1.7. Установите и настройте персональный брандмауэр (firewall) на вашем компьютере. Это позволит вам запретить несанкционированный удаленный доступ к вашему компьютеру из сети Интернет и вашей локальной сети с использованием удаленного управления компьютером и терминального доступа. Рекомендуется настроить брандмауэр на доступ только по адресам системы «ВТБ Бизнес».

1.8. Исключите запуск и работу сервисов (как встроенных в ОС, так и сторонних), позволяющих получить удаленный доступ к компьютеру, в том числе и с целью администрирования и обслуживания.

1.9. В обязательном порядке следует отключать автозапуск в операционной системе (для OS Windows: «Панель управления» -> «Администрирование» -> «Службы»; необходимо найти в закладке «Расширенный» службу «Определение оборудования оболочки» и установить «Отключено»).

1.10. На компьютере должна быть установлена только одна операционная система, и только те программы, которые необходимы в работе с ИБ «ВТБ Бизнес». Рекомендуется настроить такой режим работы, чтобы исключить запуск любых иных программ, кроме тех, которые необходимы в работе с системой «ВТБ Бизнес».

1.11. Программное обеспечение, установленное на компьютере, не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

1.12. Компьютеры должны быть защищены с помощью специальных программных или аппаратных средств антивирусной защиты (сетевых или персональных) и сетевой защиты (персональные фаерволы), разрешающие доступ к сети Интернет только тем программам, которые необходимы для работы с системой «ВТБ Бизнес» и запрещающие любое несанкционированное обращение к компьютеру из сети Интернет.

1.13. Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты вашего компьютера – программы поиска шпионских компонент, программы защиты от «спам»-рассылок.

1.14. Не рекомендуется использовать компьютер, с которого ведется работа в системе «ВТБ Бизнес», для иных целей. Исключите посещение с компьютеров сайтов сомнительного содержания и любых других Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов от недостоверных источников.

1.15. Категорически не рекомендуется работать с системой «ВТБ Бизнес» с Устройств, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.), т.к. это существенно увеличивает риск кражи ваших персональных данных.

1.16. Регулярно производите обновления антивирусных баз, а также обновления по безопасности прикладного программного обеспечения, установленного на компьютере (включая обновление антивирусных систем, фаервола, офисных программных приложений и т.п.), а также обновления операционной системы.

1.17. Не следует исполнять и открывать файлы, полученные из сети Интернет или через съемные носители, без проведения предварительной их проверки на предмет содержания в них программных закладок и вирусов.

1.18. На компьютере должна быть установлена парольная защита на вход в UEFI либо BIOS и в операционную систему. При выборе пароля необходимо следовать следующим рекомендациям:

- пароль должен содержать не менее 8 и не более 10 символов;
- в числе символов пароля должны присутствовать латинские буквы и цифры, специальные символы (@, #, $, &, *, % и т.п.) использовать нельзя;

не используйте в качестве пароля имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об администраторе или пользователе;

- не используйте в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов и общепринятые сокращения (например, («USER», «TEST» и т.п.);
- не используйте в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567» или «1йфячыц2» и т. п.);
- используйте в качестве пароля комбинацию знаков, смысл последовательности которых трудно определить;
- при смене пароля новое значение не должно совпадать ни с одним из 5 последних ранее используемых паролей;
- не используйте функции автосохранения паролей в браузерах;
- не передавайте пароли по каналам связи (например, по электронной почте) в открытом виде;
- при вводе пароля исключите возможность его подсматривания посторонними лицами и фиксирование фото/ видеокамерами;
- изменяйте пароль доступа к ИБ «ВТБ Бизнес» не реже 1 раза в 3 месяца.

1.19. Настройку компьютера (управлению привилегиями, квотами, установке прав доступа пользователей и т.п.) должен выполнять специалист, обладающий необходимыми навыками по администрированию компьютерной техники и сети.

1.20. Перечень пользователей, имеющих доступ к компьютеру, должен быть ограничен. Права пользователя, работающего с системой «ВТБ Бизнес», на данном компьютере должны быть минимально необходимыми (наличие прав администратора должно быть запрещено).

2. Требования по обеспечению безопасности при хранении и использовании Ключевой информации

2.1. Использование Средств электронной подписи и Ключевой информации допускается в целях, определенных в Договоре системы «ВТБ Бизнес».

2.2. Храните Ключевую информацию на отдельных Ключевых носителях (флешки, USB-токены и тп.). Храните Ключевые носители в надежном месте, исключающем доступ к ним неуполномо-

ченных лиц. Рекомендуется для хранения использовать надежные металлические хранилища.

2.3. В течение рабочего дня вне времени составления передачи и приема ЭД, а также по окончании рабочего дня Ключевые носители (если Ключевая информация хранится на отдельных носителях) необходимо помещать в хранилище.

2.4. Установка Ключевых носителей на рабочее место допускается только непосредственно на время работы с системой «ВТБ Бизнес». После окончания сеанса работы в системе «ВТБ Бизнес» съемный Ключевой носитель должен быть незамедлительно извлечен из компьютера.

2.5. Если Вы используете несколько Ключей ЭП при работе в системе «ВТБ Бизнес», не переносите эти Ключи ЭП на один Ключевой носитель, а также не подключайте одновременно различные Ключевые носители к компьютеру. Банк не рекомендует изготовление дубликатов Ключей ЭП.

2.6. Для контроля доступа к съемному Ключевому носителю установите на него пароль. Не сообщайте никому пароль для доступа к съемному Ключевому носителю (включая работников Банка и работников вашей организации или ваших родственников).

2.7. Не допускается:

- снимать несанкционированные копии с Ключевого носителя;
- знакомить с содержанием Ключевого носителя или передавать Ключевой носитель лицам, к ним не допущенным;
- выводить Ключи ЭП на дисплей компьютера или принтер;
- устанавливать Ключевой носитель в считывающее устройство компьютера, программные средства которого функционируют в непредусмотренных (нештатных) режимах, а также на другие компьютеры;
- записывать на Ключевой носитель постороннюю информацию.

2.8. В случае компрометации Ключей ЭП должна быть проведена их замена.

2.9. Генерацию ключей ЭП осуществляйте лично с записью Ключевой информации на съемный Ключевой носитель. Не допускайте копирования сгенерированных Ключей ЭП.

2.10. Производите замену Ключей ЭП до истечения срока их действия. Кроме того, проводите замену Ключей ЭП во всех случаях увольнения и/или смены лиц, имеющих доступ к системе «ВТБ Бизнес», а также Уполномоченных лиц Клиента, и в случае подозрений на их компрометацию.

2.11. После окончания работы в системе «ВТБ Бизнес» обязательно корректно завершите работу (выйдите из системы «ВТБ Бизнес» с использованием кнопки «Выход») и/или закройте используемый браузер.

3. Требование к соблюдению правил безопасности при использовании средств доступа (логинов/ паролей)

3.1. Логины и пароли для работы в системе «ВТБ Бизнес» – это ваша персональная конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте свой логин и пароль никому, включая работников Банка. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения, лиц с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова, и т.д.) ни при каких обстоятельствах не следует сообщать данную информацию.

3.2. Не сохраняйте ваш логин и пароль в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.

4. Требование к соблюдению правил безопасности при работе в системе «ВТБ Бизнес»

4.1. При работе с системой «ВТБ Бизнес» убедитесь, что защищенное соединение по протоколу https установлено именно с официальным сайтом услуги (https://lite.vtb.ru, https://db.vtb.ru). Настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка www.vtb.ru) или поступивших по электронной почте писем.

4.2. Обращайте внимание на любые изменения в привычных для вас процессах установления соединения с системой «ВТБ Бизнес» или в функционировании системы «ВТБ Бизнес». При возникновении любых сомнений в правильности функционирования системы «ВТБ Бизнес» незамедлительно обратитесь в Банк.

4.3. При использовании механизма импорта документов из каталогов общего доступа необходимо обеспечить безопасность данных каталогов. Права доступа к данным каталогам должны

быть минимально необходимыми для обеспечения транспортного функционала. Документы, загруженные из каталогов общего доступа, должны обязательно проходить стадию визуального контроля пользователем.

4.4. Если вы подозреваете, что пароль доступа к системе «ВТБ Бизнес» стал известен посторонним лицам, немедленно смените его.

4.5. В случае утраты Ключевого носителя, утраты ключей от хранилища в момент нахождения в нем Ключевого носителя, а также в случае возникновения ситуации, связанной с временным доступом неуполномоченных лиц к Ключевому носителю либо в связи с подозрением, что такой доступ имел место, необходимо незамедлительно обратиться в Банк в связи с компрометацией Ключа ЭП.

4.6. В случае появления предупреждений браузера о перенаправлении вас на другой сайт при подключении к системе «ВТБ Бизнес», отложите совершение операций и обратитесь в контакт-центр Банка.

4.7. В случае сбоев в работе компьютера или его поломки во время работы в системе «ВТБ Бизнес» или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска, обнаружено заражение компьютера вредоносными программами, возникли сомнения в правильности функционирования системы, появились платежные документы, которые вы не формировали и т.п.), следует немедленно извлечь Ключевой носитель и выключить компьютер, а также обратиться в Банк и убедиться, что от вашего имени не производились несанкционированные операции (путем сверки операций за день).

4.8. Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте работникам Банка обо всех подозрительных или несанкционированных операциях.

4.9. Незамедлительное обращение в Банк с предоставлением полной информации о несанкционированном списании денежных средств со счетов может позволить оперативно приостановить транзакцию и предотвратить финансовые потери.

5. Требования по обеспечению безопасности при использовании Мобильного устройства, простой электронной подписи и правила защиты SIM-карты

При использовании Мобильного устройства для доступа к системе «ВТБ Бизнес» существуют угрозы мошеннических атак. Актуальность данных угроз обусловлена как наличием многочисленных уязвимостей мобильных платформ, так и упрощением сценариев работы пользователей с Мобильными приложениями. При работе с данными устройствами необходимо соблюдать ряд требований по обеспечению конфиденциальности информации, хранящейся на данных устройствах, а также информации, доступ к которой осуществляется с использованием данных устройств. Для минимизации рисков информационной безопасности при использовании мобильных устройств необходимо:

5.1. Устанавливать приложение и его обновления только через официальные магазины: Google Play, Apple Store, AppGallery. Установка приложений из сторонних источников должна быть запрещена.

5.2. Не использовать внешние ссылки с других ресурсов для входа в официальный магазин для установки приложений, вход осуществлять только через иконку магазина в Мобильном устройстве.

5.3. Установить на свое Мобильное устройство антивирус и регулярно обновлять его.

5.4. Своевременно устанавливать обновления операционной системы, Мобильного приложения и других приложений на вашем Мобильном устройстве.

5.5. Исключить использование взломанных Мобильных устройств с активированными правами суперпользователя (root для Android платформ или jailbreak – для IOS платформ).

5.6. Использовать только лицензионное программное обеспечение.

5.7. Не подключать Мобильное устройство к не доверенному компьютеру.

5.8. Обеспечить конфиденциальность своих учетных данных в системе «ВТБ Бизнес» – логина, пароля и одноразовых OTP-кодов подтверждений, не передавать их третьим лицам, не хранить их в открытом доступе.

5.9. Обеспечить отсутствие доступа третьих лиц к Мобильному устройству и SIM-карте, посредством которых осуществляется доступ к номеру телефона, используемого при работе в системе «ВТБ Бизнес» (в том числе для формирования ПЭП), в том числе с использованием штатных средств ограничения доступа (PIN-код, графический ключ, Touch ID, Face ID и т.п).

5.10. Активировать автоблокировку Мобильного устройства с установкой пароля для доступа к рабочему столу ОС (PIN-код, графический ключ, Touch ID, Face ID и т.п), в этом случае при утере им никто не сможет воспользоваться.

5.11. Не открывать ссылки и SMS-сообщения на Мобильном устройстве, полученные от неизвестных вам лиц.

5.12. Не подключаться к общедоступным Wi-Fi сетям.

5.13. При использовании почтового клиента не использовать опцию «запомнить пароль».

5.14. Обеспечить сокрытие отображения текстов SMS/ PUSH-сообщений на заблокированном Мобильном устройстве.

5.15. Не хранить на Мобильном устройстве конфиденциальную информацию (PIN-коды платежных карт, пароли для доступа к системе «ВТБ Бизнес» и т.п.).

5.16. Удалять конфиденциальную информацию в случае передачи Мобильного устройства другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек Мобильного устройства.

5.17. Незамедлительно производить блокировку SIM-карты в случае утери или кражи Мобильного устройства или SIM-карты и приостановить доступ к системе «ВТБ Бизнес».

5.18. Написать заявление сотовому оператору о запрете принимать обращения на блокировку/ разблокировку/ замену SIM-карты от третьих лиц по доверенности.

5.19. Использовать, по возможности, для получения OTP-кодов (кодов подтверждения) отдельное Мобильное устройство, отличное от Мобильного устройства, используемого для доступа к системе «ВТБ Бизнес».

5.20. В случае обнаружения блокировки вашей SIM-карты без вашего ведома, необходимо немедленно приостановить доступ к системе «ВТБ Бизнес», обратившись в контакт-центр Банка по телефону 8 (800) 200 77 99 или в обслуживающий офис Банка.

5.21. При использовании услуг SMS/ e-mail-информирования об операциях проверять реквизиты в направляемых Банком информационных сообщениях о проведенных операциях. В случае возникновения подозрений о мошеннических действиях незамедлительно сообщать Банку по официальному номеру телефона, указанному на сайте Банка https://www.vtb.ru.

5.22. При подписании платежного документа в системе «ВТБ Бизнес» осуществлять сверку реквизитов, полученных в SMS-сообщении с OTP-кодом подтверждения, с реквизитами документа, отображаемыми в интерфейсе системы «ВТБ Бизнес»/ Мобильном приложении.

5.23. Не допускать передачу OTP-кодов подтверждений действий в системе «ВТБ Бизнес» или совершения операций третьим лицам, в том числе работникам Банка. Работники Банка никогда не обращаются по телефону к клиентам для уточнения OTP-кода операции.

5.24. При совершении любых действий, вызывающих подозрение в совершении мошенничества, в том числе:

- при поступлении на ваше устройство OTP-кода с реквизитами операции, которую вы не совершали;
- попытке уточнения OTP-кода подтверждения по телефону, в том числе от лица работника Банка, под предлогом необходимости отмены ошибочной операции в связи с техническим сбоем системы,

необходимо незамедлительно оповестить Банк по номеру телефона, указанному на Сайте Банка в сети Интернет.

5.25. Не допускать использование SIM-карты с зарегистрированным в системе «ВТБ Бизнес» номером телефона в сетевом оборудовании общего доступа (USB-модем, роутер и тд.). При использовании SIM-карты с зарегистрированным в системе «ВТБ Бизнес» номером телефона в указанном оборудовании, возникает опасность доступа третьих лиц к передаваемой Банком в SMS - сообщениях информации, в том числе и одноразовым кодам для подтверждения действий в системе «ВТБ Бизнес.

6. Требования по обеспечению безопасности при использовании Клиентом Генератора паролей и EMV-карты

6.1. Использование Генератора паролей и EMV-карты допускается в целях, определенных в

Условиях системы «ВТБ Бизнес».

6.2. Использование Клиентом для входа в систему «ВТБ Бизнес» OTP-кода сформированного посредством Генератора паролей и EMV-карты возможно при условии наличия EMV-карты у каждого Пользователя.

6.3. Получение EMV-карты в офисе Банка должно осуществляться лично каждым Пользователем.

6.4. Генератор паролей и EMV-карту в течение рабочего дня вне времени составления передачи и приема ЭД, а также по окончании рабочего дня необходимо хранить в надежном месте, исключающем доступ к ним неуполномоченных лиц.

6.5. Не допускается:

- использовать в системе «ВТБ Бизнес» Генератор паролей, полученный вне Банка;
- подвергать Генератор паролей механическим воздействиям, приводящим к повреждению экрана, разъема для карты, порче батарейки;
- хранить ПИН вместе с EMV-картой;
- передавать EMV-карту и ПИН третьему лицу;
- переподключать EMV-карту в системе «ВТБ Бизнес» другому Пользователю.

6.6. В случае компрометации Генератора паролей и/или EMV-карты должна быть произведена их замена.